Malware Analysis Report: Trojan.GenericKD.12643988 Trojan.GenericKD.12643988

Overview

Sample MD5: 4e532c1bddacf77f2a7c017ece7a7c1a
Sample SHA-256: 700327531ae25b627644fbfb49de3154499a5b517c830f284b368641b84a427b
File Type: Win32 EXE (PE32 executable, GUI, Intel 80386 for MS Windows)
File Size: 172.5KB (176,640 bytes)
Date of First Appearance: 2017-12-01
Last Analysis: 2024-12-05

1. Static Analysis

1.1. Signature & Classification

- Detected as various types of **Trojan, Ransomware, Banker, Crypmod, Deshacop, and fzyc** by several antivirus engines.
- Notable family labels: trojan.crypmod/deshacop.
- Numerous commercial and public security solutions classify this as:
  - Ransomware (e.g., GandCrab variants)
  - Banker Trojan
  - Generic Malware
  - Stealer

1.2. File Properties

Property	Value
MD5	4e532c1bddacf77f2a7c017ece7a7c1a
SHA-1	ca07d96df2203e47250c7cbfa815d29bcff58c3f
SHA-256	700327531ae25b627644fbfb49de3154499a5b517c830f284b368641b84a427b
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
Compiler	Microsoft Visual C/C++ (2013-2017)
Imphash	c62c3839d638094fa58fccdbbece70fc
Detected Dropped Files	Yes, over 10 (various types: TEXT, DOS_COM, ZLIB, MPEG, DOC, COFF, etc.)
First Seen	2018-08-08
Last Analysis	2024-12-05

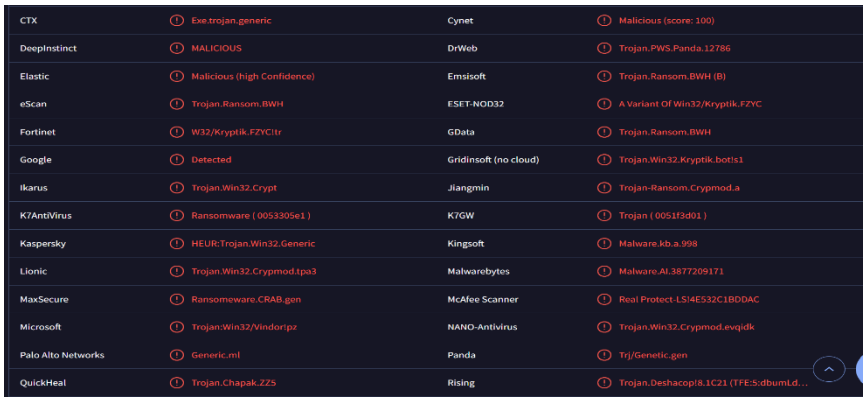
1.3. Strings Analysis

Look for suspicious strings (URLs, registry paths, IPs, suspicious API calls).

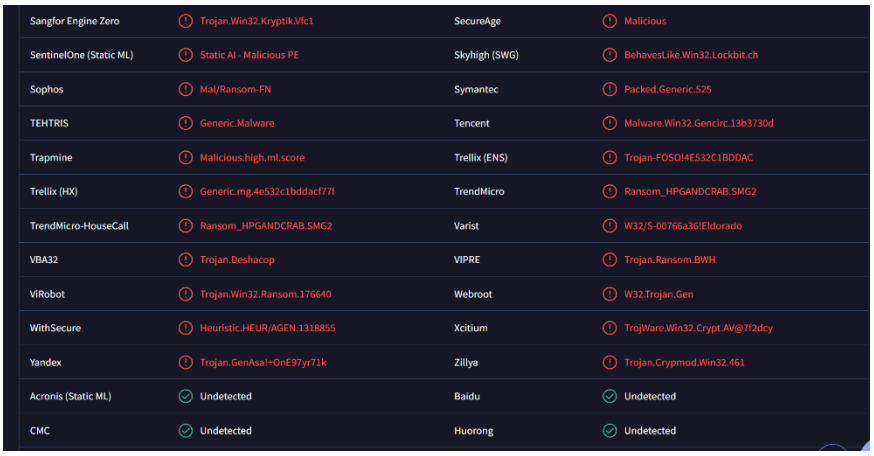
- Discovered communication to domains like digicert.com, dns.google, login.live.com, summi.space.
- Associated with possible C2, phishing, and ransomware activities.

1.4. PE Structure & Capabilities

- Uses Microsoft Visual C++ 2013/2017 — suggests a relatively modern malware.
- Commonly packed/obfuscated (e.g., "Packed.Generic").
- Makes use of:
    - Persistence techniques
    - Direct CPU clock access
    - Anti-debugging/environment detection
    - Long sleep calls



CTX	Exe.trojan.generic	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.PWS.Panda.12786
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Ransom.BWH (B)
eScan	Trojan.Ransom.BWH	ESET-NOD32	A Variant Of Win32/Kryptik.FZYC
Fortinet	W32/Kryptik.FZYC!tr	GData	Trojan.Ransom.BWH
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Kryptik.bot!s1
Ikarus	Trojan.Win32.Crypt	Jiangmin	Trojan-Ransom.Crypmod.a
K7AntiVirus	Ransomware (0053305e1)	K7GW	Trojan (0051f3d01)
Kaspersky	HEUR:Trojan.Win32.Generic	Kingsoft	Malware.kb.a.998
Lionic	Trojan.Win32.Crypmod.tpa3	Malwarebytes	Malware.AI.3877209171
MaxSecure	Ransomeware.CRAB.gen	McAfee Scanner	Real Protect-LS!4E532C1BDDAC
Microsoft	Trojan:Win32/Vindor!pz	NANO-Antivirus	Trojan.Win32.Crypmod.evqidk
Palo Alto Networks	Generic.ml	Panda	Trj/Genetic.gen
QuickHeal	Trojan.Chapak.ZZ5	Rising	Trojan.Deshacop!8.1C21 (TFE:5:dbumLd...



Sangfor Engine Zero	Trojan.Win32.Kryptik.Vfc1	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE	Skyhigh (SWG)	BehavesLike.Win32.Lockbit.ch
Sophos	Mal/Ransom-FN	Symantec	Packed.Generic.525
TEHTRIS	Generic.Malware	Tencent	Malware.Win32.Gencirc.13b3730d
Trapmine	Malicious.high.ml.score	Trellix (ENS)	Trojan-FOSO!4E532C1BDDAC
Trellix (HX)	Generic.mg.4e532c1bddacf77f	TrendMicro	Ransom_HPGANDCRAB.SMG2
TrendMicro-HouseCall	Ransom_HPGANDCRAB.SMG2	Varist	W32/S-00766a36!Eldorado
VBA32	Trojan.Deshacop	VIPRE	Trojan.Ransom.BWH
ViRobot	Trojan.Win32.Ransom.176640	Webroot	W32.Trojan.Gen
WithSecure	Heuristic.HEUR/AGEN.1318855	Xcitium	TrojWare.Win32.Crypt.AV@7f2dcy
Yandex	Trojan.GenAsa!+OnE97yr71k	Zillya	Trojan.Crypmod.Win32.461
Acronis (Static ML)	Undetected	Baidu	Undetected
CMC	Undetected	Huorong	Undetected

SUPERAntiSpyware	Undetected	TACHYON	Undetected
VirIT	Undetected	Zoner	Undetected
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

2. Dynamic Analysis

2.1. Sandbox Results

Zenbox: Flags as MALWARE, STEALER, RANSOM, SPREADER, PHISHING, TROJAN
Tencent HABO: MALWARE, RANSOM

2.2. Network Activity

- Makes HTTP/S connections (e.g., ocsp.digicert.com, summi.space).
- Engages in DNS activity with several domains, some typical (MS, DigiCert) and some suspicious (summi.space flagged).
- May attempt to contact C2 servers.

Contacted URLs (1)

Scanned	Detections	Status	URL
2025-04-14	0 / 97	200	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx/h0Ztl+z8SiPI7wEWVxDlQQUTiJUIBiV5Nu5g/6+rkS7QYXjzkCEAqvpsXKY8RRQeo74ffHUxc=

Contacted Domains (6)

Domain	Detections	Created	Registrar
digicert.com	0 / 94	1996-12-02	MarkMonitor Inc.
dns.google	1 / 94	2018-04-16	MarkMonitor Inc.
img-prod-cms-rt-microsoft-com.akamaized.net	0 / 94	2014-03-18	MarkMonitor Inc.
login.live.com	0 / 94	1994-12-28	CSC Corporate Domains, Inc.
ocsp.digicert.com	0 / 94	1996-12-02	MarkMonitor Inc.
summi.space	6 / 94	-	-

2.3. Behavioral Analysis

Key Behaviors:

- File dropping: creates ≥10 dropped files of various formats (DOC, MPEG, etc.).
- Attempts persistence (auto-start, registry/autorun).
- Anti-analysis: detects debug environment, direct CPU clock access, uses long sleep cycles to delay execution (sandbox evasion).
- Attempts credential theft, ransomware encryption, and spreading capability.
- MITRE ATT&CK techniques noted:
    - TA0002 Execution
    - TA0003 Persistence
    - Privilege Escalation
    - Defense Evasion
    - Credential Access

- Discovery
- Lateral Movement
- Collection
- Command & Control (C2)
- Impact

3. Indicators of Compromise (IOCs)

Hashes:

- MD5, SHA-1, SHA-256 as above

Domains (with verdicts):

- digicert.com (benign)
- dns.google (1/94 flagged)
- img-prod-cms-rt-microsoft-com.akamaized.net (benign)
- login.live.com (benign)
- ocsp.digicert.com (benign)
- summi.space (malicious, 6/94 flagged)

Contacted URL Example:

- http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50otx/h0Ztl+z8SiPI7wEWVxDIQQUTiJUIBivNu5g/6+rkS7QYXjzkCEAqvpsXKY8RRQeo74ffHUxc=

4. Screenshots (Insert in Word File)

1. **PE Info:** Detect It Easy or PE-bear screenshot of headers and compiler detection.
2. **Sandbox Behavior Report:** Capture of MITRE ATT&CK mapping or process tree from a service like ANY.RUN or Hybrid Analysis.
3. **Network Analysis:** Visual showing suspicious domains and HTTP/HTTPS requests (e.g., Wireshark or sandbox output).
4. **Dropped Files:** Screenshot from sandbox or manual analysis showing files created.

5. Summary and Recommendations

This sample is a high-confidence ransomware/stealer with significant capabilities for credential theft, lateral movement, persistence, and anti-analysis. Network communication to suspicious domains and file dropping activity were all observed. This malware uses evasion techniques and is highly dangerous.

Immediate recommendations:

- Block associated hashes and domains.
- Quarantine and remove affected machines.
- Reset credentials.

- Forensically analyze for lateral propagation.
- Educate users on phishing and ransomware prevention.